REMARKS/ARGUMENTS

Favorable reconsideration of this application, as presently amended and in light of the following discussion, is respectfully requested.

Claims 1-19 are currently pending in the present application.

In the outstanding Office Action, Claims 1, 2, 4-8, 10-15, and 17-19 were rejected under 35 U.S.C. §103(a) as unpatentable over Eliott (U.S. Patent No. 6,468,160); and Claims 3, 9, and 16 were rejected under 35 U.S.C. §103(a) as unpatentable over Eliott in view of Chan (U.S. Patent No. 6,473,860).

In a non-limiting embodiment of the claimed invention, first and second communication paths are set up as different channels on an identical transmission line or as different transmission lines, where the first transmission path is used for communications other than transfer of the executable programs and the second transmission path is used for transfer of the executable programs. The first communication path is an ordinary communication path between the program distribution device (server) and the client device. The second communication path is a dedicated special communication path that directly connects the program distribution device (server) and the tamper resistant processor within the client device.

Claim 1 recites, *inter alia*,

> a first communication path set up unit configured to set up a first communication path between the program distribution device and the client device for communications other than transfer of the executable programs;
>
> a second communication path set up unit configured to set up a second communication path directly connecting the program distribution device and the tamper resistant processor for transfer of the executable programs, the first and second communication paths being set up as different channels on an identical transmission line or as different transmission lines.

The outstanding Office Action takes the position that Eliott discloses the claimed first and second communication paths at col. 26, lines 37-62, and col. 27, lines 20-48. Applicants respectfully traverse this position.

Col. 26, lines 37-62, of Eliott only describes exchanges of user name, password, authentication information, session information, etc., between the user's browser and the Internet service provider's server, without mentioning a communication path used for this purpose.

Furthermore, col. 27, lines 20-48 of Eliott only describes downloading the control information from the server to the disk drive controller, so as to securely control disk partitions that are created, and to control which applications have access to respective partitions. Although Eliott states that a direct security link exists between server 101 and a disk drive controller resident within the expansion device 95, this direct security link is to be realized by the Internet security features, such as RSA's secure socket layer, firewalls, etc. There is no disclosure or suggestion of any specific communication path used for the purpose of securely controlling disk partitions that are created and controlling which applications have access to respective partitions.

Furthermore, the disk drive controller is merely a digital signal processor associated with the hard drive in the expansion device 95, and it is not a processor for executing programs (applications) in the video game system 50, which is the user's device.

Eliott does not disclose or suggest that the disk drive controller 50 is a tamper resistant processor. In this regard, in col. 25, lines 35-63 quoted in the outstanding Office Action, Eliott only mentions a security check (or security authentication) between the security processor 180 and the security processor associated with the hard drive 206. Such a security check (security authentication) between processors has absolutely nothing to do with a physical property of a processor itself. Eliott completely fails to disclose or suggest any processor that is tamper resistant.

Eliott fails to disclose or suggest any teaching or suggestion for utilizing a dedicated special communication path that directly connects the program distribution device (server) and the tamper resistant processor within the client device, specifically for the purpose of distributing executable programs to a type of the client device that has the tamper resistant processor provided inside.

Claim 1 also recites

> an encryption processing unit configured to produce an encrypted program by encrypting an executable program to be distributed to the client device and executed within the tamper resistant processor, by using the unique public key of the tamper resistant processor; and

> a transmission unit configured to transmit the encrypted program to the tamper resistant processor through the second communication path so that the encrypted program is directly delivered to the tamper resistant processor and the encrypted program can be decrypted and executed only within the tamper resistant processor which is an only entity that has the unique secret key corresponding to the unique public key.

The outstanding Official Action takes the position that the above-noted features of Claim 1 are disclosed in col. 25, lines 15-40, col. 26, lines 18-37, col. 25, lines 14-24 and 29-63, and col. 29 lines 5-17 of Eliott. Applicants respectfully traverse this position.

Col. 25, lines 15-40, 14-24, and 29-63 of Eliott only describes the encryption of the game software by the server 101 using the private encryption key transmitted to the server 101 in encrypted form. Col. 26, lines 18-37 of Eliott only describes the encryption of the video games resident on hard drive 206 by the server using the unique ID as a key. Col. 29, lines 5-17 of Eliott only describes the encryption of downloaded game software by the server 101 using the encryption key unique to each individual hard drive 206.

Eliott completely fails to describe any public key that is uniquely assigned to a processor or a use of such a public key for the purpose of encrypting a program.

Thus, Eliott fails to disclose or suggest encrypting an executable program by using the unique public key of the tamper resistant processor such that the encrypted program can be decrypted and executed only within the tamper resistant processor which is an only entity that has the unique secret key corresponding to the unique public key.

Applicants note that these two features (i.e., encrypting the program by using the public key of the tamper resistant processor and transmitting the encrypted program through the claimed "second communication path) are combined in the claimed invention in a specific way to realize a specific technical effect. Applicants respectfully submit that a separate showing of each one of these features cannot obviate the claimed invention. Namely, a combination of the feature of encrypting the program by using the public key of the tamper resistant processor and the feature of transmitting the encrypted program through the second communication path, of a type as discussed above, has the significant technical effect of ensuring that the encrypted program is directly delivered to the tamper resistant processor and the encrypted program can be decrypted and executed only within the tamper resistant processor which is an only entity that has the unique secret key corresponding to the unique public key.[1] Eliott fails to disclose any teaching or suggestion for such a specific combination of these features for the purpose of realizing such a technical effect.

In view of the above-noted distinctions, Applicants respectfully submit that Claim 1 (and Claims 2-6 dependent thereon) patentably distinguish over Eliott. Claims 7, 13, and 14 are similar to Claim 1. Applicants respectfully submit that Claims 7, 13, and 14 (and Claims 8-12, and 15-19 dependent thereon) patentably distinguish over Eliott for at least the reasons provided for Claim 1.

Consequently, in view of the above amendments and comments, it is respectfully submitted that the outstanding rejection is overcome and the pending claims are in condition for allowance. An early and favorable action to that effect is respectfully requested.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Eckhard H. Kuesters
Attorney of Record
Registration No. 28,870

Joseph Wrkich
Registration No. 53,796

Customer Number
22850

Tel: (703) 413-3000
Fax: (703) 413 -2220
(OSMMN 06/04)

[1] Specification, page 19, lines 6-14